

A METHOD FOR PERFORMING A HAZARD REVIEW AND SAFETY  
ANALYSIS OF A PRODUCT OR SYSTEM

BACKGROUND OF THE INVENTION

[0001] This invention relates to safety analysis of a product or system. More particularly, it relates to a method for conducting an analysis of a product or a system to evaluate risk(s) to personnel or equipment and identify mitigating conditions that may control or avoid such risks.

[0002] A variety of different processes have been used in the past to determine safety of various systems. These processes are often introduced after the occurrence of a catastrophic event or after the occurrence of a consistent series of events resulting in harm to personnel.

[0003] Preliminary hazard assessment (PHA) had origins from a combination of generic industry hazard checklists. These checklists required identification of inherent hazards, which a test applicant must address specifically in a subsequent review session. One of the shortcomings of this process involves the task of addressing the risk that was left entirely to an applicant - in any style deemed appropriate to the applicant's knowledge. Thus, the documentation of the approach and the results greatly varied and required additional time and resources to ensure completeness. Also, gathering information with respect to critical hazardous features and combinations depended on an initial reviewer's expertise.

[0004] Hazard characterization and personal safety analysis involves examination of hazards associated with a job or a task. In this technique, workers are grouped so that risks and exposures experienced by any member of a group are representative of the group as a whole. Information about the nature of a workplace, equipment and materials used, and the tasks to be performed may be considered as the basis of this step.

[0005] In another approach, a preliminary assessment of hazards require a minimal effort to identify the inventory of hazardous materials to perform an initial hazard categorization. Reviewing basic facility information on intended facility operations and using estimates of materials may lead to an acceptable assessment. Hazard characterization also uses information from existing hazard analysis documentation such as, for example, safety analysis reports, process hazard analysis, job safety analysis (JSA), and the job hazard analysis.

[0006] Hazards are identified and resultant risks are assessed by considering probability of occurrence and severity of consequence. System safety is part of the overall program risk management decision process. Severity is an assessment of the worst potential consequence, defined by degree of injury or property damage, which could occur. For example, hazard severity may be categorized as: catastrophic, critical, marginal and negligible.

[0007] Factors for identification of hazards include, for example, (a) identification of hazardous components, (b)

identification of hazardous operating conditions, (c) safety related interface considerations, (d) environmental constraints including operating environments, (e) training and certification pertaining to hazardous and safety critical operations and maintenance of hazardous and safety critical systems, etc.

[0008] Hazardous operations review analysis is performed to evaluate activities for hazards or risks introduced into a system by operational and support procedures and also to evaluate the adequacy of operational and support procedures that are used to eliminate or control identified hazards or risks. Typically, hazards are identified and evaluated by considering such criteria as plan system configuration and state at each phase of an activity; facility interfaces; supporting tools including software controlled automatic test equipment, to name but a few. Human factor(s) may be considered as an element of the total system, receiving both inputs and initiating outputs during the conduct of the analysis.

[0009] Safety efforts related to the hazardous operations review process focus primarily on the safe operation of a system. This process focuses on the operational phase of the system with specific emphasis on single-point failures. This process is not easily implemented for multiple system and multiple point failures.

[0010] There is a need for a structured, standardized and efficient methodology for conducting a thorough analysis of a single product or a complex system to evaluate

risk(s) to personnel and equipment, and identify mitigating factors to reduce the identified risk(s).

#### BRIEF DESCRIPTION OF THE INVENTION

[0011] The present invention provides a structured, standardized and efficient methodology for conducting a effective analysis of a product or a complex system to evaluate the risk to personnel and equipment safety. Further, the present invention identifies and implements mitigating factors to control possible risks to personnel and equipment.

[0012] The safety review process methodology of the present invention combines preliminary hazard assessment, hazardous operations review, and accident scenario review processes into a unique systemic series of actions. The present method further provides the flexibility to invoke and execute the safety review process at almost any stage in the development of a new product, or the use of an existing product.

[0013] Specifically, the present method analyzes, using a preliminary hazard assessment, a system or product to identify inherent hazards associated with the system or product. Of the inherent hazards, those hazards that are safety-comprising are identified in a hazardous operations review. Safety-compromising hazards are analyzed to rate the severity of the potential unsafe condition. Predetermined and established operating parameters of the product are considered, along with deviations from those established operating parameters. With respect to a deviation for an operating parameter,

the possible safety consequences of the deviation are considered. This process is repeated until all the factors contributing to credible single-point failures and unsafe conditions are considered.

[0014] A system or product is also evaluated for a multi-system or multi-point failure using an accident scenario review, if an identified unsafe condition is of sufficient severity, is associated with a plurality of components of the system or is associated with various distinct systems. In this case, a thorough analysis of mitigating factors is performed to stop progression of the risk(s). Additional control measures are adopted to further reduce the likelihood of potential hazards from occurring. This process is repeated until the overall risk level is found to be acceptable.

[0015] An embodiment of the present invention is a method for analyzing a system for safety to personnel or other systems, said method comprising: a) segmenting a product into subcomponents for hazard review; b) identifying at least one operating parameter of a first subcomponent of said product; c) identifying an inherent hazard of said first subcomponents based on an analysis of the at least one operating parameter; d) identifying features of the structure or operation of the subcomponent corresponding to the inherent hazard; e) identifying modifications or controls for the identified features which would mitigate the inherent hazard; f) prioritizing the identified features with respect to the effect that each of said features has on safety of the product; g) identifying current documentation that defines the structure or operation of the subcomponent; h) including in the

current documentation, a safety audit procedure that identifies one or more of said prioritized features for inspection, and i) determining whether an unsafe condition could result from the inherent hazard after step (e).

[0016] This embodiment of the invention may further include a method, wherein an unsafe condition has been determined, for conducting a hazardous operation review comprising: j) identifying at least one contributing factor to the unsafe condition, where said factors are selected from a group comprising at least one of: a design deviation of the subcomponent, an operating mode of the subcomponent, and a mode of personal interaction with the subcomponent; k) generate a matrix correlating the identified features and the contributing factors, wherein the matrix identifies the at least one contributing factor corresponding to each of the identified features; l) create a hazardous operation table that identifies for each of said identified features a cause of the corresponding contributing factor and the modifications and controls to mitigate the hazard; m) determining a risk of the hazard based on a severity level of the unsafe condition corresponding to the hazard and a likelihood of an occurrence of the hazard; n) if the risk exceeds a predetermined level, identifying further modifications or controls for the identified features which would mitigate the inherent hazard, and then repeating the determination of risk step until the risk is no greater than the predetermined value or no further modifications or controls are identifiable.

[0017] The embodiment of the invention may further include a method further comprising an accident scenario review, if after step (n) the possible severity exceeds the predetermined level, said accident scenario review comprising: o) identifying one or more of the inherent hazards contributing to the unsafe condition; p) generating a logical path of steps leading from the identified inherent hazards to an accident occurring due to the unsafe condition, wherein the logical path is generated using the hazardous operations table; q) identifying the steps of the logical path that, if avoided, would prevent the accident; r) for each identified step, assign a likelihood level of a probability that the step will occur, and s) if the likelihood level for the identified step exceeds a predetermined threshold, identifying modifications or controls which would mitigate the inherent hazard.

[0018] A second embodiment of the invention is a method for analyzing a system for safety to personnel or other systems, said method comprising: a) segmenting a product into subcomponents for hazard review; b) identifying an inherent hazard of a first subcomponents; c) determining whether an unsafe condition may result from the hazard and assigning a severity level to the unsafe condition; d) determining a risk of the hazard based on the severity level of the unsafe condition corresponding to the hazard and a likelihood of an occurrence of the hazard; e) issuing control actions to mitigate the identified hazard; f) terminating the method if the determined severity level is no greater than the predetermined severity level; g) devising an accident scenario based on the unsafe conditions and the identified hazard; h)

repeating steps (a) to (g) until the determined risk of the hazard leading to an unsafe condition and resulting harm is within predetermined levels.

[0019] A third embodiment of the invention is a method of evaluating a product for safety, said method comprising: a) determining if the product can be analyzed as a single component, and if true; b) identifying single-point failures likely to cause a hazard; c) reviewing product design features likely to cause the hazard; (d) identifying unsafe conditions contributing to the hazard; (e) assigning a severity level to each of the unsafe conditions of the hazard; (f) completing the method if the severity level of each of the unsafe conditions is no greater than a predetermined threshold severity level; (g) if one or more of the severity level of one or more of the unsafe conditions is greater than the threshold severity level, performing an accident scenario review; and h) identifying and issuing mitigating actions to prevent one or more of the unsafe conditions.

[0020] The third embodiment may further include: determining overall risk level of the product; comparing the overall risk level with predetermined risk level value; and storing risk related data if the overall risk level is within predetermined risk level value.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIGURE 1 is a high-level block diagram of a safety review process.



[0022] FIGURES 2 to 4 are of a high level flowchart to identify and mitigate hazards related to a product or system in accordance with an exemplary embodiment of the present invention.

[0023] FIGURES 5 and 6 are of a detailed flowchart illustrating the process steps to identify preliminary hazards associated with a product or system in accordance with an exemplary embodiment of the present invention.

[0024] FIGURES 7 to 9 are of a detailed flowchart illustrating the process steps to perform hazard operations review further to identifying preliminary hazards associated with a product/system in accordance with an exemplary embodiment of the present invention and as illustrated in FIGURE 3.

[0025] FIGURES 10 to 13 are a detailed flowchart illustrating the process steps identifying multi-point failures and determining if the overall risk is acceptable in accordance with an exemplary embodiment of the present invention.

[0026] FIGURE 14 is a high level flowchart showing a modified process, as shown in Figures 2 to 4, in which single and multipoint failures are evaluated.

[0027] FIGURE 15 illustrates a system and process to store in a database the results of a safety review.

#### DETAILED DESCRIPTION OF THE INVENTION

[0028] FIGURE 1 is a block diagram of a three-step safety review process to evaluate hazards for a product, system or method (collectively referred to as the product). In a first step 10, the product is segmented into sub-systems or sub-components, if necessary. Each sub-system or sub-component 12 is individually analyzed for safety using a three-step process that generally includes a preliminary hazard assessment 14, hazardous operations review 16 and an accident scenario review. The hazard assessment 12 and hazardous operations review 14 may be applied individually to each sub-system 12, and the accident scenario review 18 may be applied to the product as a whole. The preliminary hazard assessment may be conducted as a "brainstorming session" 20 to identify the inherent hazards associated with the product and its operation. A determination is made as to whether any of the inherent hazards might become a safety compromising hazard. If a credible safety compromising hazard is identified, the process proceeds to a hazardous operation review. Using the results of the preliminary hazard assessment 14, a listing of hazardous operations may be generated and defined as a straw-man HAZ-OP table 22. Accident scenarios 25 are considered to identify the cause and effect of identified hazards. The hazardous operations taken from table 22 are analyzed in the review process 16. Straw-man accident scenarios 24 are prepared based on the results of the hazardous operation review 16 if the hazardous operation review identifies a resulting unsafe condition of high severity. The straw-man table 22 and straw-man accident scenario 24 may be prepared by "facilitator(s)", who may be independent of the persons conducting the safety review for each sub-system and oversee the entire review process.

[0029] A safety review team may comprise the following persons:

[0030] Facilitator: A person(s) charged with ensuring that the safety review process steps are followed, the documentation is kept in a consistent manner, and ensuring that the meetings are focused on relevant subject matter.

[0031] Owner: A person(s) having technical ownership of a product. The owner has responsibility of providing technical understanding of the subject (product or process or system), and is authorized to implement direct change to the product or process if necessary. Additional owners from other sub-systems or components that interface with the present system, may also be required. For example, interface owners may come from quality control, manufacturing, sourcing, transport, etc. and are deemed necessary to cover critical to safety topics.

[0032] Reviewers: People with experience in the field(s) associated with the subject. Reviewers are charged with having expertise in technical, legal, environmental, health and safety issues, to name a few. The members of the review team provide necessary checks and balances in reviewing the hazards associated with the subject. Reviewers also assure critical review of the controls and verifications that are in place to mitigate the hazards of a subject. Further, reviewers provide state-of-the-art knowledge capability to implement additional controls or verifications.

[0033] FIGURES 2 to 4 show a high-level flow-chart 26 illustrating an overall hazard review and safety process comprising steps to identify inherent hazards of a product and determine if the measured risk level due to the identified hazards is within predetermined risk levels. Once inherent hazards are identified, single-point failures based on each identified hazard are determined. If the determined risk level is within predetermined values, those values are documented. However, if the determined risk level is not within predetermined values, then mitigating factors to control the single-point failures are identified.

[0034] A determination is then made to identify if a hazard is related to a high severity, unsafe condition. Such conditions may be the result of multi-point failures, e.g., when a hazard spans several sub-systems or components of a product. If a high severity, unsafe condition is identified, then a thorough analysis of the affected sub-systems or components of the product is performed and mitigating factors to prevent the high severity, unsafe condition are determined. A further determination is made to identify if the overall risk level of a product under review is acceptable or not. If the overall risk level is found to be acceptable, then such information is documented and the method ends. If not, the process is repeated until the overall risk level is found to be within acceptable limits.

[0035] The overall hazard review and safety process shown in Figures 2 to 4 is grouped into a preliminary hazard review sub-process 28, a hazardous operations review sub-process 30, and an accident scenario review sub-process

32. Each of these sub-processes are described in further below and in connection with the additional figures.

[0036] At the completion of the hazardous operations review, a determination is made as to whether the current identified severity level of the identified unsafe condition(s) is greater than a pre-defined critical level 34. The predefined critical level is set by the facilitator, owners, reviewers and/or by company standard. If the identified unsafe conditions are no greater than the critical level of severity, the overall hazard review and safety process is documented and completed. The overall process is terminated based on a recognition that there is an acceptable level of hazard risk. Some remaining level of risk cannot be easily avoided and exists in all safe products and safe systems. Once this acceptable level of hazard risk is achieved, the overall process is completed and the product or system may be deemed safe. However, if the unsafe condition has a high severity rating, then the hazard review and safety process continues to the accident scenario review 32.

[0037] FIGURES 5 and 6 show a detailed flowchart illustrating the process steps for the sub-process of the preliminary hazard assessment 28 that identifies inherent hazards associated with a product in accordance with an exemplary embodiment of the present invention. The preliminary step of this process 28 determines if a product may be analyzed as a unit, or whether the product should be analyzed in sub-systems or sub-components. During the preliminary hazard assessment, a structured brainstorming activity may be performed to highlight

inherent hazards associated with the product. During this initial step, second objectives may also be collected. The second objectives assist in determining the features of the product that are already in place that mitigate risks and control inherent hazards. This step of obtaining secondary objectives may be accomplished by working through the format of a questionnaire.

[0038] An exemplary questionnaire may ask owners to describe in detail the product, or its sub-system and components, using drawings, diagrams, tables, or other descriptors. This process may familiarize or re-familiarize the owners and the reviewers of the product. The owners of the product may then have to go through a pre-assembled list of generic inherent hazards tailored to the industry or the product field. During this familiarization step, the owners may work with a facilitator to identify generic inherent hazards related to the product. The resulting tailored list allows the owners to focus only on relevant hazards. Typically, there may be three life cycle categories that the hazards may occur. Examples of life cycle categories include installation, operation, maintenance for industrial equipment, and manufacture, use, disposal for a consumer product. A determination is made to identify the relevant portion of the life cycle of the product or system, where the hazard may occur. The description of how the hazard occurs may be determined via a group discussion. Additionally, the cause of the hazard and current known features that are in place in order to control or mitigate the hazard may be listed.

[0039] During the preliminary hazard assessment step, the owners of a product may be asked to summarize the key safety assuring goals associated with the subject product or system. This step may result in a concise statement as to how identified risks need to be controlled or mitigated. For example, the primary safety critical factor of a pressure vessel is to retain structural integrity over time. This desirable feature may be ensured through attention to creep failure margins of the vessel during the design process. Following the step of identifying the key safety control and mitigation features, the owners may be asked to list other components, sub-systems that interact with the subject product in order to determine if the other sub-systems are affected by the hazards identified with respect to the current sub-system. A list is also created identifying the current documentation which includes, for example, design practices, industry codes and standards, instruction manuals, and other documentation that are currently used to control the subject product or system.

[0040] The owners are asked to list key items that can be verified as a final check in order to ensure that safety features are established and in place. These are typically known as operational readiness review items (ORR). Examples of ORR may include a pop-up button on the sealed food container, a red tag on a safety critical aerospace feature, or a correctly run vent line on an industrial fuel system.

[0041] FIGURES 7 to 9 show a detailed flowchart illustrating the process steps to perform the sub-process of hazard operations review 30 that further identifies

safety comprising hazards associated with a product. The second set of the safety review process methodology performs hazardous operations review drawing initial information from the preliminary hazard assessment. During this step, parameters or deviations based upon the basic operating parameters of a product or system are identified in order to determine off design or single-point failure mechanisms that might result in safety issues.

[0042] The facilitator may assemble information necessary to create an intermediate or strawman hazardous operations table from a preliminary hazardous assessment document. During this step, various product parameters and deviations from these parameters that may compromise the safety of the product or system are identified. In the event that the severity level of the associated unsafe condition is above a critical level, the safety review process methodology of the present system is expected to perform a third additional step of the accident scenario review in their review as illustrated in Figure 10 to 13.

[0043] The basic operating parameters of a specific product usually make up the primary parameters responsible for potential hazards. Subsequently, for each parameter, a deviation or a set of deviation words are chosen for some off design or unintended situations.

[0044] The basic operating parameters and their deviations are usually based on a single-point failure mechanism that a review team is expected to consider. The strawman hazardous operations table is completed ahead of the



hazardous operations review process to the extent possible with additional information from the owner of the product in addition to the preliminary hazard assessment format. The step of creating a strawman hazardous operations table may increase the efficiency of a review team meeting. A formal review is then executed with a review team working stepwise through the straw-man table confirming or altering the figures identifying parameter, deviation, cause, consequence (e.g. the unsafe condition), controls, and verifications relating to a hazard. The review team, upon reviewing each raw entry in the hazardous operations table, rates the severity of the potential unsafe condition that may occur. The review team then determines the likelihood of the consequence occurring given the current controls and verifications that are in place. In order to maintain consistency with other review processes, the safety review process of the present invention involves "severity" and "likelihood" ratings related to an existing standard.

[0045] After obtaining a ranking score or risk level for each single-point failure, the review team then determines if the current safety ranking of each single-point failure is adequate or whether further control or mitigation steps are required. If it is determined that further control or mitigation steps are deemed necessary, the required steps are recorded in an action item assigned to a person to mitigate the potential risks. After the action item is assigned and executed, the safety review team determines if a reduction in severity or likelihood of hazard occurrence has occurred. This information is recorded and stored.

[0046] During the hazardous operations review process, if an unsafe condition is determined to have a severity level above the predefined critical level, then an accident scenario review (ASR) step is required to adequately assure the safety of the overall product or system. This additional step is often required when direct human interaction is considered. In determining whether to proceed with this additional ASR step, the safety review team may be required to decide whether the severity is high enough to warrant further effort to reduce hazards. The severity rating of the unsafe condition may be recorded first before the accident scenario review is assembled.

[0047] FIGURES 10 to 13 show a detailed flowchart illustrating the process steps for the sub-process accident scenario review (ASR) 32 that identifies high severity failures that may involve multiple single point failures, and determines if the overall risk is acceptable. The ASR step provides a detailed final analysis in order to allow an understanding of the steps that lead to a high severity unsafe condition, and an understanding of the inter-related safety critical features that are in place in order to stop the progression of the scenarios leading to the unsafe condition.

[0048] The contributory hazard steps are identified that may lead to the unsafe condition. These steps are most often a series of single-point failures identified during the hazardous operation review. Additional human factor steps, such as, confusion over switches or lack of

training, may be taken into account in determining contributory hazard steps.

[0049] During each step of this ASR process, the controls and verifications, which may be identical to the control and verification steps as identified with respect to the hazardous operations review step, may be listed. At each ASR step, the review team determines the likelihood of progressing to the next step.

[0050] As a final consensus, the safety review team determines at the end of ASR process, whether the scenario as a whole is adequately controlled, and whether the overall-risk level is acceptable. If the overall risk level is unacceptably high, then actions are considered to increase controls or verifications that may reduce the risk level. If the risk level is unacceptable and further controls or verifications do not reduce the risk, the redesigning of the product may be considered. If the overall risk level is acceptable, information obtained in the ASR process is documented and stored. This information may be used as a template in the event of future changes to a product, or when similar products are created.

[0051] Figure 14 is a high level flowchart showing a modified process in which single and multipoint failures are evaluated. After conducting a preliminary hazard assessment 28, a hazardous operations review 40 is conducted which is similar to the review shown in Figures 7 to 9, but includes a step 42 for identifying single failures of the product, and determining whether each single point failure will result in one of the identified

inherent hazards. For each single point failure, and especially for those that may cause a hazard, features of the product, e.g., product components or operational steps of the product, are identified that could be modified to prevent or mitigate the single point failure, in step 44.

[0052] During the accident scenario review, step 46, the modified process identifies and evaluates multipoint failures of the product, step 48, that may lead to an unsafe condition. A multipoint failure is, for example, a condition where two or more structural parts of a product fail or whether two or more standard operating procedures for the product do not occur or are preformed improperly, or some combination of failures of parts and procedures. Potential multipoint failures may be identified by considering the likelihood that two or more of the identified potential single point failures could occur together and result in an unsafe condition, that would not have resulted due to any one of the single point failures alone.

[0053] For the multipoint failures that result in a new unsafe condition (which are identified in step 48), an identification, step 50, is made of the features of the products, e.g., parts and operations, which may be modified to prevent or mitigate the unsafe condition resulting from the multipoint failure. If the overall risk of the product is not acceptable after step 50, then additional features are identified and considered, step 52, to reduce the risk level of the product. With these newly identified features, the hazardous operation review 40 process is repeated.

[0054] Figure 15 shows an exemplary system schematic to perform the method steps described above and save the results of the safety review. The product 60 readied for the safety review and a search is performed in a computer database of documentation regarding prior safety reviews, step 62. If a previous safety review conducted on a similar product is in the database, then the documentation of the safety review is obtained and review in preparation for the safety review of the new product 60. Prior safety reviews provide information on hazards, unsafe conditions, failure points and mitigating factors of similar products. This information may be helpful in performing a safety review of a new product. With the documentation from prior review, a new safety review 64 is performed in accordance with the procedures shown in the preceding figures. If at the conclusion of the safety review, the safety of the product is deemed acceptable, step 66, then the documentation of the safety review process is stored in the computer database for future use. But if the product is not sufficiently safe, then additional mitigating factors are evaluated, step 68, and the product review is repeated.

[0055] A structured framework to evaluate hazards is described herein with standardized documentation to create a universal, efficient, comprehensive approach in analyzing a product to assure necessary safety requirements. Also provided is a clearly structured, simple format for the safety review that ensures a rigorous treatment of the product. It ensures efficiency, by focusing the available limited time and resources on the most severe safety hazards. The present method also uses standardized tables for documentation to

enhance clarity and thereby provide a basis for future product enhancements. It also defines sources of safety hazards inherent to a product or a system. Further, total risks are defined by the severity (or magnitude) of personnel injury or equipment damage that could occur and the likelihood of occurrence.

[0056] In addition to the above, means to determine whether the current risk level is acceptable is provided by identifying key features that assure acceptability. Also identified are those items that need to be better controlled to ensure an acceptable risk level. These items are identified by performing highly detailed risk analysis into specific unsafe conditions that, due to their high severity, require better control to ensure an acceptable risk level.

[0057] The present safety review process also provides for documenting a company's diligent efforts to understand and control safety risks associated with the company product, thus providing a clear record for ensuring that safety is designed and built into future products.

[0058] The safety review process methodology of the present invention may be applied to any industry, product or process. The safety review process methodology of the present invention may be best administered by a focused group of facilitators in order to ensure commonality of documentation and standardization of record keeping. This method provides the ability to quickly search and identify previous similar templates when considering a new product, thus ensuring a consistent flow of the process over time and across product lines. A

categorized database may be created to store the complete records of the hazard review process. This assists in performing such searches.

[0059] While the invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not to be limited to the disclosed embodiment, but on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.